DWeb Weekend 2025 - Saturday 8/16/2025

Roundtable Discussion 1.4

Title: What can we do without personal identifiers?
Time: 11:15 - 12:00
Attendees: Micah, Liam, Ben, Dmitri, Michael, Tiffany, Matthew, YT
Note taker: Ying Tong

Please add your /initials/ at the front of a comment

General Notes

- [Micah] Inspired by Backchannel, which works without identifiers
    - no way to spam / impersonate
    - everything happens through local names / nicknames
    - provocation: what applications can we build on this?
- [Liam] Do personal identifiers have to mean global identifiers, or just relative? e.g. posts on an anonymous bulletin board cannot be attributed to the same person
- [Micah] Somewhere between anonymous and fully identifiable; the process of association between people is localised and relational
- [Ben] At least one identifier per relationship
- [Micah] In Backchannel, an identifier is a shared symmetric key
- [Ben] Existing standard: DIDPeer https://identity.foundation/peer-did-method-spec/ (https://identity.foundation/peer-did-method-spec/)
- [Michael] How pragmatic is it to have one identifier for each relationship? e.g. in group settings, or if I want to introduce two friends
- [Micah] In Backchannel, association features are left "up to the reader"; one way could be to generate a "linking token" that is passed to multiple friends

- [Michael] We could have versions of identifiers?
- [Ben] Connecting is riskier if I have to share my global username with the counterparty
- [Liam] We could use repudiable attestations
- [Michael] In practice, this is equivalent to centralised services you could use anonymously
- [Micah] It's similar, but missing many social tools e.g. "@ mention" feature
- [Micah] A "linking token" is a way to link two aliases; you could reveal a linking name to everyone in the group chat
- [YT] A "linking token" is a pointer, but not a shared key; how would we generate a shared key for a group chat?
- [Matt] A group chat could be realised through an invite link
- [Liam] Can the validity of a linking token be proven to a third party?
- [YT] Symmetric encryption, messages are completely forgeable, as are links and social graphs
- [Liam] Real-world application: I want to convince my landlord of my relationship with the bank, but don't want my landlord to be able to prove this to someone else
- [Ben] Some novel schemes are using threshold keys for relationship identifiers
- [Ben] Which schemes are doing this well right now? DID peer allows two DIDs to come up with a DID that represents their relationship
- [Dmitri] Chris Allen, DID peer using FROST
- [Dmitri] First-person credentials is a proposed solution for proof of personhood using mutual signatures
- [Michael] Privacy issue: how to prove reputation without revealing identity
- [Dmitri] We need some sort of external reputation engine that is resilient against sharing; we need to have negative consequences for a spammer
- [YT] Is there inherent tension between privacy and reputation? e.g. Backchannel has no Sybil resistance
- [Micah] We could augment Backchannel

- [Dmitri] We need some kind of trust anchor & chain of signature
- [Micah] There is some kind of trust in establishing a shared channel, i.e. that the counterparty will not share the key with a third person
- [Dmitri] OCapN protocol provides a way to bootstrap a transitive capability?
- [YT & Dmitri] Clouds of social relations say nothing about reputation; need external trust anchors
- [Tiffany] Transitive trust is imperfect
- [Dmitri] Excited for UI innovations that communicates information about transitive trust
- [Micah] "Gather-apply-scatter" is the graph equivalent of MapReduce, reputation based on PageRank
- [YT] Is it computationally difficult to distinguish a fake social graph from a real one?
- [Ben] We need revocation as well, Backchannel not sufficient, need OCapN

Summary to be reported to the other DWeb Weekend participants

a)

b)

c)

name of the reporter